APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/585,358	06/02/2000	Atsushi Maeda	500.38618X00	6526

20457   7590   06/03/2004

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-9889

EXAMINER
ZAND, KAMBIZ

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/585,358	MAEDA ET AL.
	Examiner	**Art Unit**	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 April 2004</u>.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 5-15* is/are pending in the application.

    4a) Of the above claim(s) *5-15* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *5-15* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>04/05/2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1.   Newly submitted claims 5-15 are directed to an invention that is independent or

distinct from the invention originally claimed for the following reasons: Claims 1-3 drawn

to a system for managing public key in an environment having a hierarchical network

with a domain name at each hierarchy, having a DNS server provided for each

hierarchy classified in class 380, subclass 285. However the newly claims 5-11 drawn to

an apparatus connectable to a network having control unit for packet transmission with

respect to a domain name and its associated public key classified in class 713/201.

Since applicant has received an action on the merits for the originally presented

invention, this invention has been constructively elected by original presentation for

prosecution on the merits. Accordingly, claims 5-11 are withdrawn from consideration

as being directed to a non-elected invention. See 37 CFR 1.142(b) and MPEP §

821.03.

2.   The text of those sections of Title 35,U.S.Code not included in this section can be

found in the prior office action.

3.   The prior office actions are incorporated herein by reference. In particular, the

observations with respect to claim language, and response to previously presented

arguments.

4.   Claim 4 have been cancelled.

5.   Claims 1-3 have been amended.

6.   Claims 1-3 are pending.

7.   Examiner withdraws objection to the drawings and specification due to correction by the applicant. The approval of formal drawings submitted by Applicant (paper number 9) have been acknowledged.

8.   Examiner withdraws rejection of claim 3 under 35 U.S.C 112-second paragraphs due to correction by the applicant.

9.   Examiner withdraws objection of claim 4 under 37 CFR 1.75 due to cancellation of the claim by the applicant.

Claim Objections

10.   Claim 3 is objected to because of the following informalities: typo error. Line 4 of claim 3 refers to "DMS server". Examiner suggests "DNS server". Appropriate clarification or correction is requested.

Response to Arguments

11.   Applicant's arguments with respect to the claims 1 and 3 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

12.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

13.   **Claims 1 and 3** are rejected under 35 U.S.C. 103(a) as being unpatentable over

Perlman (5,455,865 A) in view of Zdepski et al (5,825,884 A).

As per claim 1 Perlman (5,455,865 A) teach a system having a hierarchical network

(see fig.1, 7a-b; col.2, lines 33-36 where a hierarchical network is disclosed) with a

domain name and address at each hierarchy (see fig.3a,4a,6a-b and 8a where each

source or node of hierarchical network has a domain name and unique address

represented by source id's; col.5, lines 31-40); and database for storing the public key

(see col.5, lines 34-40 where a memory is an storage for storing data and where

allocation of the public key and unique id's and other information in lines 41-57 is the

database of each node since the database is nothing but a space within an storage area

where information is kept) comprising having an inquiry from a first host to the second

host to obtain information on the public key of the second host; triggering a response by

sending the information on public key of the second host to the first host (see col.5,

lines 58-67; col.6, lines 1-11 where by using a handshake the request for inquiry and

the response is being taken place and where each node transmit the public key

requested by the other node in order to identify themselves to each other) but do not

disclose a DNS server provided at each hierarchy where the DNS server distribute a

public key of a host to the host belongs to the network. However Zdepski et al

(5,825,884 A) disclose a DNS server provided at each hierarchy where the DNS server

distribute a public key of a host to the host belongs to the network (see fig.2, item 276;

fig.5; col.2, lines 24-31; col.5, lines 64-67 and col.6, lines 1-20 where the database

server that stores subscribers public keys and their ids corresponds to DNS server that

stores public keys and by handshaking and request and challenge communicate with

other hosts to provide request service based on association of the public key stored and

its association with the id of the other host). It would have been obvious to one of

ordinary skilled in the art at the time the invention was made to utilize Zdepski et al's

public key database within a server in Perlman's hierarchical network in order to

provide protection for certain proprietary database interacting with other segments of

the interactive environment.

As per claim 3 Perlman (5,455,865 A) teach a method for managing a public key as

claimed in claim 1, wherein said host provides means for inquiring said server of the

public key of another host (see col.5, lines 58-67; col.6, lines 1-11 where by using a

handshake the request for inquiry and the response is being taken place and where

each node transmit the public key requested by the other node in order to identify

themselves to each other); and means serving to inquire said server of the

corresponding public key to the domain name of the target host when security communication is started (see fig.4b,5a and 5b where means for inquiry with respect to corresponding information are disclosed based on the communication between the nodes) but do not disclose a DNS server provided at each hierarchy where the DNS server distribute a public key of a host to the host belongs to the network. However Zdepski et al (5,825,884 A) disclose a DNS server provided at each hierarchy where the DNS server distribute a public key of a host to the host belongs to the network (see fig.2, item 276; fig.5; col.2, lines 24-31; col.5, lines 64-67 and col.6, lines 1-20 where the database server that stores subscribers public keys and their ids corresponds to DNS server that stores public keys and by handshaking and request and challenge communicate with other hosts to provide request service based on association of the public key stored and its association with the id of the other host). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Zdepski et al's public key database within a server in Perlman's hierarchical network in order to provide protection for certain proprietary database interacting with other segments of the interactive environment.

14.   **Claims 1 and 3** are rejected under 35 U.S.C. 103(a) as being unpatentable over Perlman (5,455,865 A) in view of Sistanizadeh et al (5,790,548 A) and further in view of Zdepski et al (5,825,884 A).

As per claim 1 Perlman (5,455,865 A) teach a system having a hierarchical network

(see fig.1, 7a-b; col.2, lines 33-36 where a hierarchical network is disclosed) with a

domain name and address at each hierarchy (see fig.3a,4a,6a-b and 8a where each

source or node of hierarchical network has a domain name and unique address

represented by source id's; col.5, lines 31-40); and database for storing the public key

(see col.5, lines 34-40 where a memory is an storage for storing data and where

allocation of the public key and unique id's and other information in lines 41-57 is the

database of each node since the database is nothing but a space within an storage area

where information is kept) comprising having an inquiry from a first host to the second

host to obtain information on the public key of the second host; triggering a response by

sending the information on public key of the second host to the first host (see col.5,

lines 58-67; col.6, lines 1-11 where by using a handshake the request for inquiry and

the response is being taken place and where each node transmit the public key

requested by the other node in order to identify themselves to each other) but do not

disclose a DNS server. However Sistanizadeh et al (5,790,548 A) disclose a network

having more than one DNS server (see col.2, lines 58-64). It would have been obvious

to utilize Sistanizadeh et al's DNS servers in different location within Perlman's

hierarchical network in order to provide hosts resolution addresses to the users such as

translation of the domain names into IP addresses. However Perlman in view of

Sistanizadeh et al do not disclose DNS server that also holds public key database. On

the other hand Zdepski et al (5,825,884 A) disclose a server provided at each hierarchy

where the server distribute a public key of a host to other host belongs to the network

(see fig.2, item 276; fig.5; col.2, lines 24-31; col.5, lines 64-67 and col.6, lines 1-20

where the database server that stores subscribers public keys and their ids corresponds

to DNS server that stores public keys and by handshaking and request and challenge

communicate with other hosts to provide request service based on association of the

public key stored and its association with the id of the other host). It would have been

obvious to one of ordinary skilled in the art at the time the invention was made to utilize

Zdepski et al's public key database within a server in Perlman's hierarchical network in

view of Sistanizadeh et al DNS server in order to provide protection for certain

proprietary database interacting with other segments of the interactive environment.

As per claim 3 Perlman (5,455,865 A) teach a method for managing a public key as

claimed in claim 1, wherein said host provides means for inquiring said server of the

public key of another host (see col.5, lines 58-67; col.6, lines 1-11 where by using a

handshake the request for inquiry and the response is being taken place and where

each node transmit the public key requested by the other node in order to identify

themselves to each other); and means serving to inquire said server of the

corresponding public key to the domain name of the target host when security

communication is started (see fig.4b,5a and 5b where means for inquiry with respect to

corresponding information are disclosed based on the communication between the

nodes) but do not disclose a DNS server. However Sistanizadeh et al (5,790,548 A)

disclose a network having more than one DNS server (see col.2, lines 58-64). It would

have been obvious to utilize Sistanizadeh et al's DNS servers in different location within

Perlman's hierarchical network in order to provide hosts resolution addresses to the

users such as translation of the domain names into IP addresses. However Perlman in

view of Sistanizadeh et al do not disclose DNS server that also holds public key

database. On the other hand Zdepski et al (5,825,884 A) disclose a server provided at

each hierarchy where the server distribute a public key of a host to other host belongs

to the network (see fig.2, item 276; fig.5; col.2, lines 24-31; col.5, lines 64-67 and col.6,

lines 1-20 where the database server that stores subscribers public keys and their ids

corresponds to DNS server that stores public keys and by handshaking and request and

challenge communicate with other hosts to provide request service based on

association of the public key stored and its association with the id of the other host). It

would have been obvious to one of ordinary skilled in the art at the time the invention

was made to utilize Zdepski et al's public key database within a server in Perlman's

hierarchical network in view of Sistanizadeh et al DNS server in order to provide

protection for certain proprietary database interacting with other segments of the

interactive environment.

Allowable Subject Matter

15.   Claim 2 is objected to as being dependent upon a rejected base claim, but would

be allowable if rewritten in independent form including all of the limitations of the base

claim and any intervening claims.

Conclusion

16.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure:

    U.S.Patent No. US (5,833,810A) teach electronic online commerce card with

    transaction proxy number for online transactions.

    U.S.Patent No. US (5,870,475 A) teach facilitating secure communications in a

    distribution network.

    U.S.Patent No. US (6,023,507 A) teach automatic remote computer monitoring

    system.

    U.S.Patent No. US (5,422,953 A) teach personal date/time notary device.
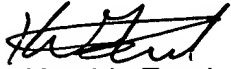

17.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Kambiz Zand whose telephone number is (703) 306-

4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts

to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the

organization where this application or proceeding is assigned as (703) 872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

06/01/2004